### (12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

### (19) World Intellectual Property Organization International Bureau



# 

### (43) International Publication Date 19 April 2001 (19.04.2001)

# **PCT**

### (10) International Publication Number WO 01/27821 A2

(51) International Patent Classification7: G06F 17/60

- (21) International Application Number: PCT/GB00/03861
- (22) International Filing Date: 6 October 2000 (06.10.2000)
- (25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data: 9923804.0

8 October 1999 (08.10.1999) GB

- (71) Applicant (for all designated States except US): HEWLETT-PACKARD COMPANY [US/US]; 3000 Hanover Street, Palo Alto, CA 94304 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): CHEN, Liqun [CN/GB]; 1 Harvest Close, Bradley Stoke, Bristol BS32 9DO (GB). BALACHEFF, Boris [FR/GB]; 7 Heathfield

Close, Keynsham, Bristol BS31 2HJ (GB). DU TOIT, Roelf [ZA/ZA]; PO Box 10705, 0046 Centurion (ZA). PEARSON, Siani [GB/GB]; 35 Sandyleaze, Westbury-on-Trym, Bristol BS9 3PZ (GB). CHAN, David [GB/US]; 16112 Mays Avenue, Monte Sereno, CA 95030

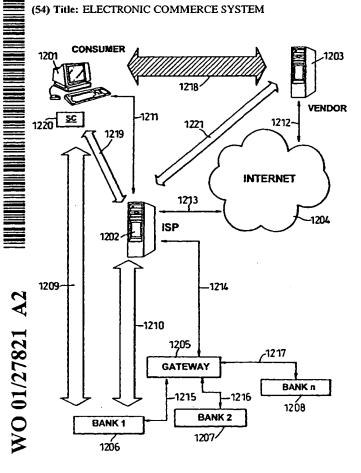
- (74) Agent: LAWRENCE, Richard, Anthony; Hewlett-Packard Limited, Intellectual Property Section, Filton Road, Stoke Gifford, Bristol BS34 8QZ (GB).
- (81) Designated States (national): JP, US.
- (84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

#### Published:

Without international search report and to be republished upon receipt of that report.

[Continued on next page]

#### (54) Title: ELECTRONIC COMMERCE SYSTEM



(57) Abstract: A method of brokering a transaction between a consumer and a vendor by a broker, wherein the consumer, the broker and the vendor are all attached to a public network, the consumer having a secure token containing a true consumer identity. The method comprising the steps of: the consumer obtaining a temporary identity from the broker by using the true consumer identity from the secure token; the consumer selecting a purchase to be made from the vendor, the consumer requesting the purchase from the vendor and providing the temporary identity to the vendor; the vendor requesting transaction authorisation from the broker by forwarding the request and the temporary identity to the broker, the broker matching the temporary identity to a current list of temporary identities, and obtaining the true consumer identity; the broker providing authorisation for the transaction based on transaction details and true consumer identity.



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/27821 PCT/GB00/03861

# **Electronic Commerce System**

This invention relates to a system for enacting electronic commerce.

- Purchasing goods using a public network, such as the Internet, plays an increasingly important role in modern society, and necessarily involves the establishment of the appropriate business relationships amongst consumers, vendors and authorisation providers.
- 10 Existing online vendors use the model described in Figure 8. This is described in greater detail below, but in summary the consumer uses the Internet Service Provider (ISP) as a connection provider and connects to the vendor's online store. The vendor is connected to the consumer's bank through a payment gateway. The payment gateway is a broker—it is used to authorise transactions and update the consumer's account. In this model the vendor will not ship the goods until it receives payment, made with a debit or credit card, which needs to be verified by or on behalf of the vendor. The distribution channel is, typically, conventional mail.

The following problems exist apply to the existing model:

- certain levels of truste exist between the consumer and the vendor, and
   between vendor and authorising bank, but these are not sufficient to satisfy all
   security concerns;
  - the consumer must to trust the platform from which the transaction is initiated, so he or she is only likely to use a platform personal to him or her;
- 25 the consumer must reveal identity and card details to the vendor;
  - the amount of effort and money needed to set up a payment gateway limits the number of vendors willing to provide an online store; and

20

25

30

- electronic goods such as software, music and videos typically need to be sent through the conventional distribution channel because of the lack of mutual trust.

Accordingly, there is provided a method of brokering a transaction between a consumer and a vendor by a broker, wherein the consumer, the broker and the vendor are all attached to a public network, the consumer having a secure token containing a true consumer identity, the method comprising the steps of: the consumer obtaining a temporary identity from the broker by using the true consumer identity from the secure token; the consumer selecting a purchase to be made from the vendor; the consumer requesting the purchase from the vendor and providing the temporary identity to the vendor; the vendor requesting transaction authorisation from the broker by forwarding the request and the temporary identity to the broker; the broker matching the temporary identity; to a current list of temporary identities, and obtaining the true consumer identity; the broker providing authorisation for the transaction based on transaction details and true consumer identity.

To address one or more of the problems of the prior art, the present inventors have proposed the method above. Embodiments of the method reduce security risks, and appropriate business relationships between consumers and vendors are set up through the use of ISPs as trusted brokers. Typically, the relationship involves a trust relationship between the broker and the consumers, and between the broker and the vendors, but not (directly) between the vendors and the consumers. Preferred embodiments of the invention involve mutual authentication and integrity checks. Particularly preferred embodiments utilise a novel method of separating payment and distribution of goods. The (financial) identity of the consumer is needed for payment, but this is revealed only to the broker and not the vendor. This does not prevent delivery of goods – electronic goods can simply be downloaded, but physical goods can be sent to the consumer's delivery address, which can be sent without compromising his financial data.

manufacture. Energy is not a combination of substances and therefore not a composition of matter.

## Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1, 2, 4, 8, 10, 13, 14, 16, 20, 23-25, 28, 29, 31, 36, and 38 are rejected under 35 U.S.C. 102(e) as being anticipated by Futa et al. [US 2003/0081771 A1], hereinafter Futa.

Regarding claim 1, Futa teaches a method comprising: generating an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve [US 2003/0081771 A1, Pg 8, Par 0154]; publishing a public key corresponding to the isogeny [US 2003/0081771 A1, Pg 1, Par 0015] [US 2003/0081771 A1, Pg 3, Par 055] [US 2003/0081771 A1, Pg 3, Par 0063]; encrypting a message using a encryption key corresponding to the isogeny [US 2003/0081771 A1, Pg 11, Par 0206]; and decrypting

the encrypted message using a decryption key corresponding to the isogeny [US 2003/0081771 A1, Pg 11, Par 0206].

Regarding claim 2, Futa teaches a method as recited by claim 1, wherein at least one of the encryption key or the decryption key is a private key [US 2003/0081771 A1, Pg 1, Par 0016], the private key being a dual isogeny of the isogeny [US 2003/0081771 A1, Pg 8, Par 0154].

Regarding claim 4, Futa teaches a method as recited by claim 1, wherein the generating maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves [US 2003/0081771 A1, Pg 10, Par 0197].

Regarding claim 8, Futa teaches a method as recited by claim 1, wherein the method signs the message [US 2003/0081771 A1, Pg 11, Par 0206].

Regarding claim 10, Futa teaches a method as recited by claim 1, further comprising composing a plurality of modular isogenies to provide the isogeny without revealing any intermediate curves [US 2003/0081771 A1, Par 0154].

Regarding claim 13, Futa teaches a method comprising: publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve [US 2003/0081771 A1, Pg 8, Par 0154] [US 2003/0081771 A1,

Pg 1, Par 0015] [US 2003/0081771 A1, Pg 3, Par 0055] [US 2003/0081771 A1, Pg 3, Par 0063]; and decrypting an encrypted message using a decryption key corresponding to the isogeny [US 2003/0081771 A1, Pg 11, Par 0206].

Claim 23 is rejected because it is similar subject matter as claim 1.

Claims 14, 24, and 29 are rejected because it is similar subject matter as claim 2.

Claims 16, 25, and 31 are rejected because it is similar subject matter as claim 4.

Claims 20, and 38 are rejected because it is similar subject matter as claim 8.

Claims 28, and 36 are rejected because it is similar subject matter as claims 13, and 10 respectively.

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

- (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
- 2. Claims 1-5, 7-17, 19-26, 28-32, and 34-39 are rejected under 35 U.S.C. 102(a) as being anticipated by Anonymous [NPL, Anonymous, November 2003].

Regarding claim 1, Anonymous teaches a method comprising: generating an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve; publishing a public key corresponding to the isogeny; encrypting a message using a encryption key corresponding to the isogeny; and decrypting the encrypted message

using a decryption key corresponding to the isogeny. [Anonymous, November 2003, Pg 1-3]

Regarding claim 2, Anonymous teaches a method as recited by claim 1, wherein at least one of the encryption key or the decryption key is a private key, the private key being a dual isogeny of the isogeny. [Anonymous, November 2003, Pg 1-3]

Regarding claim 3, Anonymous teaches a method as recited by claim 1, wherein the isogeny is generated using a technique selected from a group comprising modular generation, complex multiplication generation, linearly independent generation, and combinations thereof. [Anonymous, November 2003, Pg 5-8]

Regarding claim 4, Anonymous teaches a method as recited by claim 1, wherein the generating maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves. [Anonymous, November 2003, Pg 1-3]

Regarding claim 5, Anonymous teaches a method as recited by claim 1, wherein the decrypting is performed by bilinear pairing. [Anonymous, November 2003, Pg 4]

Regarding claim 7, Anonymous teaches a method as recited by claim 1, wherein the method is applied using Albelian varieties. [Anonymous, November 2003, Pg 1-3 --

Examiner notes that Albelian varieties are inherent in generating isogenous elliptic curves as taught by Anonymous.]

Regarding claim 8, Anonymous teaches a method as recited by claim 1, wherein the method signs the message. [Anonymous, November 2003, Pg 10]

Regarding claim 9, Anonymous teaches a method as recited by claim 1, wherein the method provides identity based encryption. [Anonymous, November 2003, Pg 11].

Regarding claim 10, Anonymous teaches a method as recited by claim 1, further comprising composing a plurality of modular isogenies to provide the isogeny without revealing any intermediate curves. [Anonymous, November 2003, Pg 7]

Regarding claim 11, Anonymous teaches a method as recited by claim 1, further comprising using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny. [Anonymous, November 2003, Pg 11]

Regarding claim 12, Anonymous teaches a method as recited by claim 1, further comprising using a trace map to shorten points on an Albelian variety. [Anonymous, November 2003, Pg 11 -- Examiner notes that an Albelian variety is inherent in generating isogenous elliptic curves as taught by Anonymous.]

Regarding claim 13, Anonymous teaches a method comprising: publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve; and decrypting an encrypted message using a decryption key corresponding to the isogeny. [Anonymous, November 2003, Pg 1-3]

Claim 23 is rejected because it is similar subject matter as claim 1.

Claims 14, 24, and 29 are rejected because it is similar subject matter as claim 2.

Claims 15, and 30 are rejected because it is similar subject matter as claim 3.

Claims 16, 25, and 31 are rejected because it is similar subject matter as claim 4.

Claims 17, 26, and 32 are rejected because it is similar subject matter as claim 5.

Claims 19, and 34 are rejected because it is similar subject matter as claim 7.

Claims 20, and 38 are rejected because it is similar subject matter as claim 8.

Claims 21, and 39 are rejected because it is similar subject matter as claim 9.

Claims 22, and 35 are rejected because it is similar subject matter as claim 11.

Claim 37 is rejected because it is similar subject matter as claim 12.

Claims 28, and 36 are rejected because it is similar subject matter as claims 13, and 10 respectively.

### Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 3, 7, 15, 19, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Futa et al. [US 2003/0081771 A1], hereinafter Futa, and further in view of Katsura [NPL, Katsura 1975].

Regarding claim 3, Futa teaches a method as recited by claim 1, wherein the isogeny is generated using a technique selected from a group comprising modular generation [US 2003/008177 A1, Pg 8, Par 0154]. Futa does not explicitly teach techniques using complex multiplication generation, linearly independent generation, and combinations thereof.

Katsura teaches generating isogenies using complex multiplication [Katsura 1975, Pg 224], linearly independent generation [Katsura 1975, Pg 226], and combinations thereof [Katsura 1975, Pg 224-228].

It would have been obvious to one of ordinary skilled in the art at the time of invention to combine the different techniques of generating isogenous curves as taught by Katsura. The suggestion/motivation for combining would have been to have various techniques for generating isogenous curves. Katsura is an analogous art because it is in the same field of generating isogenous curves.

Regarding claim 7, Futa and Katsura teaches a method as recited by claim 1, wherein the method is applied using Abelian varieties [Katsura 1975, Pg 224 --Examiner notes that an Abelian variety becomes an inherent property when performing the above techniques of generating isogenies.].

Claims 15, and 30 are rejected because it is similar subject matter as claim 3.

Claims 19, and 34 are rejected because it is similar subject matter as claim 7.

2. Claims 5, 9, 11, 17, 21, 22, 26, 35, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Futa et al. [US 2003/0081771 A1], hereinafter Futa, and further in view of Boneh et al. [US 7113594 B2], hereinafter Boneh.

Regarding claim 5, Futa teaches a method as recited by claim 1.

Futa does not teach wherein the decrypting is performed by bilinear pairing.

Boneh teaches a method for identity based encryption wherein the decrypting is performed by bilinear pairing [US 7113594 B2, Col 3, Ln 4-12].

It would have been obvious to combine identity based encryption into the encryption method of Futa utilizing an elliptic curve generating device. The suggestion/motivation is to have the flexibility of being able to send an encrypted message to a recipient whose public key has not yet been generated and published [US 7113594 B2, Col 1, Ln

51-57]. Boneh is an analogous art because it is in the field of encryption whose method can be derived from an elliptic curve when using Weil or Tate pairing.

Regarding claim 9, Futa and Boneh teaches a method as recited by claim 1, wherein the method provides identity based encryption [US 7113594 B2, Col 10, Ln 23].

Regarding claim 11, Futa and Boneh teach a method as recited by claim 1, further comprising using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny [US 7113594 B2, Col 22, Ln 27-49].

Claims 17, 26, and 32 are rejected because it is similar subject matter as claim 5.

Claims 21, and 39 are rejected because it is similar subject matter as claim 9.

Claims 22, and 35 are rejected because it is similar subject matter as claim 11.

3. Claims 6, 18, 27, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Futa et al. [US 2003/0081771 A1], hereinafter Futa, Boneh et al. [US 7113594 B2], hereinafter Boneh, and further in view of Eisentrager et al., hereinafter Eisentrager [NPL, Eisentrager November 2003].

Regarding claim 6, Futa and Boneh teaches a method as recited by claim 5, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, and Tate pairing [US 7113594 B2, Col 2, Ln 30-40].

Futa and Boneh does not teach square pairing.

Eisentrager teaches an improved Weil and Tate pairings for elliptic and hyperelliptic curves also known as the squared Weil or squared Tate pairings [Eisentrager 2003, Pg 3, 8].

It would have been obvious to one of ordinary skilled in the art at the time of invention to combine Eisentrager pairing techniques. The suggestion/motivation would have been to have an improved pairing of the predecessors as part of the selection of the various bilinear pairing techniques. Eisentrager is an analogous art because it is in the same filed of encryption whose method can be derived from an elliptic curve when using Weil or Tate pairing.

Claims 18, 27, and 33 are rejected because it is similar subject matter as claim 6.

4. Claims 12, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Futa et al. [US 2003/0081771 A1], hereinafter Futa, and further in view of Katsura [NPL, Katsura 1975].

Regarding claim 12, Futa, and Boneh teach a method as recited by claim 1, further comprising using a trace map to shorten points on an elliptic curve mapped by the isogeny [US 7113594 B2, Col 22, Ln 27-49].

Futa and Boneh does not explicity teach an elliptic curve that is an isogeny of an Albelian variety.

Katsura teaches generating an elliptic curve mapped by isogenies of an Albelian variety [Katsura 1975, Pg 224].

It would have been obvious to one of ordinary skilled in the art at the time of invention to accommodate isogenies of an elliptic curve as taught by Katsura. The suggestion/motivation would have been to have a trace map for isogenies generated by the various techniques that comprise complex multiplication, linearly independent equations, and combinations thereof as taught by Katsura. Katsura is an analogous art because it is in the same field of generating isogenous elliptic curves.

Claim 37 is rejected because it is similar subject matter as claim 12.

5. Claims 6, 18, 27, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anonymous [NPL Anonymous, November 2003], and further in view of Eisentrager et al., hereinafter Eisentrager [NPL, Eisentrager November 2003].

Regarding claim 6, Anonymous teaches a method as recited by claim 5, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, and Tate pairing [Anonymous, November 2003, Pg 4].

Anonymous does not explicitly teach square pairing.

Eisentrager teaches an improved Weil and Tate pairings for elliptic and hyperelliptic curves also known as the squared Weil or squared Tate pairings [Eisentrager 2003, Pg 3, 8].

It would have been obvious to one of ordinary skilled in the art at the time of invention to combine Eisentrager pairing techniques. The suggestion/motivation would have been to have an improved pairing of the predecessors as part of the selection of the various bilinear pairing techniques. Eisentrager is an analogous art because it is in the same filed of encryption whose method can be derived from an elliptic curve when using Weil or Tate pairing.

Claims 18, 27, and 33 are rejected because it is similar subject matter as claim 6.

# Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/ Martin Jeriko San Juan Examiner. Art Unit 2132

/Gilberto Barron Jr/ Supervisory Patent Examiner, Art Unit 2132